UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

Michael Duane Hoffman,

Defendant.

Criminal No. 13-107 (DSD/FLN)

REPORT AND RECOMMENDATION

Nathan Petterson, Assistant United States Attorney, for Plaintiff.
Frederic K. Bruno for Defendant.

THIS MATTER came before the undersigned United States Magistrate Judge on June 5, 2013 on the defendant's suppression motions (ECF Nos. 21 & 22). The matter was referred to the undersigned pursuant to 28 U.S.C. § 636 and Local Rule 72.1. The government called one witness at the hearing, Minneapolis Police Officer Dale Hanson, and entered three exhibits into evidence.[1] Both parties submitted additional briefing after the hearing. For the reasons set forth below, the Court recommends that the defendants' motions be **DENIED**.

I. FINDINGS OF FACT

Officer Dale Hanson is a police officer with the Minneapolis Police Department who does computer and cell-phone forensic work on several task forces involving child exploitation, including the Internet Crimes Against Children Task Force. Transcript, ECF No. 30, at 11. On February 19,

[1] The government's exhibit 1 is an application for a search warrant, a supporting affidavit, the search warrant, and a return. The government's exhibit 2 is an audio recording of an interview that Officer Hanson conducted with the defendant at his home during the execution of the search warrant. The government's exhibit 3 is a transcript of the first five minutes of the interview.

2013, Officer Hanson obtained a warrant to search the defendant's residence in Red Wing, Minnesota. *Id.*

The application in support of the search warrant described an investigation conducted by Officer Hanson between November and December 2012.[2] Gov.'s Ex. 1. Using a computer program called Ephex, Officer Hanson connected to various peer-to-peer file sharing networks. ECF No. 30 at 32. The Ephex program, which is available only to law enforcement, maintains a list of IP addresses previously identified by investigators as possessing or sharing possible child pornography. ECF No. 30 at 20, 32–33. Once connected to a file-sharing network, the Ephex program searches the network to see if any of the suspected IP addresses are online. *Id.* at 32. If so, the Ephex program attempts to connect with the computer associated with that IP address. *Id.* Once a connection is established, the Ephex opens another program called Phex. *Id.* Phex is a publicly available program. *Id.*

On November 16, 2012, Officer Hanson connected to a peer-to-peer file-sharing network called Gnutella2 using the Ephex program. *Id.* at 20, 29; Gov.'s Ex. 1 at "pg. 4." Like other peer-to-peer file sharing networks, any member of the public who has a computer and access to the internet can download the software that enables him to connect to the Gnutella2 network. ECF No. 30 at 30; Gov.'s Ex. 1 at "pg 2." Gnutella2 gives its users the ability to search for and download files from other users. Gov.'s Ex. 1 at "pg 2." It also allows a user to make files on his computer available to other users, typically by placing it in a designated "shared" folder. *Id.* If a user wants to find a file on Gnutella2, he must enter a keyword search into the search box in the program. *Id.*

[2] At the hearing on the defendant's motions to suppress, Officer Hanson further explained some of the technology described in his search-warrant affidavit.

The server returns a list of files that match the search criteria. *Id.* The user then double-clicks the file and initiates a download directly from the computer of whichever user made the file available for download. *Id.*

On November 16, 2012 Officer Hanson directly connected with a computer using the IP address 24.179.159.158 on the Gnutella2 network.[3] ECF No. 30 at 20, 23; Gov.'s Ex. 1 at "pg. 4." Through two administrative subpoenas, Officer Hanson later discovered that the IP address belonged to the defendant. Gov.'s Ex. 1 at "pg. 17." Officer Hanson's program generated a list of 117 files shared by the defendant's computer, of which 51 were "investigative files of interest." Gov.'s Ex. 1 at "pg. 4." Officer Hanson downloaded 10 of these files directly from the physical hard drive on the defendant's computer. Gov.'s Ex. 1 at "pg. 4." He continued to download additional "investigative files of interest" from the defendant's computer on multiple occasions between November 16 and December 25, 2012. *Id.* at "pg. 4–18." Officer Hanson visually confirmed that the files contained digital images of child pornography. Gov.'s Ex. 1 at "pg. 16-18." The warrant affidavit contains a detailed description of ten of the images he downloaded from the defendant's computer. *Id.* at "pg. 16–18."

On the basis of the information described above, Officer Hanson obtained a warrant authorizing the search of the defendant's residence. Gov. Ex. 1. The warrant was executed on February 21, 2013, and the defendant was present at his residence during the search. ECF No. 30 at 11–12. Officer Hanson conducted a recorded interview with the defendant at that time. Gov.'s

[3] Officer Hanson testified that the program used by the IP address 24.179.159.158 to connect to the Gnutella2 network is called Shareaza. ECF No. 30 at 28. The Shareaza program allows a user to connect to multiple file-sharing networks, including Gnutella2, simultaneously. *Id.* at 30.

Ex. 2. At the beginning of the interview, Officer Hanson informed the defendant that he was not under arrest, was free to leave, and was not going to jail. Gov.'s Ex. 2 at 2. The defendant acknowledged that he understood he was not under arrest and was free to leave. *Id.* at 2–3. He then made several inculpatory statements. Gov.'s Ex. 3.

II. CONCLUSIONS OF LAW

The defendant contends that Officer Hanson violated the Fourth Amendment when he directly connected to the defendant's computer and downloaded images from it without a warrant or a valid exception to the warrant requirement. He asserts that any evidence seized pursuant to the search warrant must be suppressed because it is the fruit of the illegal searches. The Court disagrees.

The Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized." If the defendant moves "to suppress evidence on the basis of an alleged unreasonable search, the defendant has the burden of showing a legitimate expectation of privacy in the area searched." *United States v. Stults*, 575 F.3d 834, 842 (8th Cir. 2009) (internal quotations and citation omitted). "Whether a defendant has a constitutionally protected expectation of privacy involves a two-part inquiry—the defendant must show that (1) he has a reasonable expectation of privacy in the areas searched or the items seized, and (2) society is prepared to accept the expectation of privacy as objectively reasonable." *Id.*

The Eighth Circuit has held that a defendant has no reasonable expectation of privacy in files that he makes accessible to others using a peer-to-peer file-sharing network. *Id.* at 843. The file-

sharing network at issue in *Stults* was LimeWire, but it functions the same as Gnutella2—the file-sharing network in this case. *Id.* at 842. The defendant cannot have a reasonable expectation of privacy in any files in a computer folder that he makes accessible to the entire world. *Id.* at 843. "One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking." *Id.* Because the defendant did not have an objectively reasonable expectation of privacy in the files he made accessible to others while using the Gnutella2 network, Officer Hanson's downloading of those files did not constitute a search within the meaning of the Fourth Amendment.[4] The defendant's motion to suppress any evidence seized pursuant to the search warrant must be denied.

III. RECOMMENDATION

Based on the foregoing, and all the files, records, and proceedings herein, it is **HEREBY RECOMMENDED** that:

1. Defendant's motion to suppress evidence obtained as a result of search and seizure (ECF No. 21) should be **DENIED**.

2. Defendant's motion to suppress defendant's statements, admissions, and answers (ECF No. 22) should be **DENIED**. The defendant did not submit any briefing on this motion after the hearing and therefore appears to have abandoned it.

DATED: June 27, 2013

s/ Franklin L. Noel
FRANKLIN L. NOEL
United States Magistrate Judge

Pursuant to the Local Rules, any party may object to this Report and Recommendation by filing with

[4] The defendant contends that this case is distinguishable from *Stults* in that there is no evidence in the record that the defendant knew that the some of his files were accessible to others. The defendant misstates the record. In his interview with Officer Hanson, the defendant indicated that he was aware he had shared files on the file-sharing network. Gov.'s Ex. 2 at 11:55 to 12:05.

the Clerk of Court and serving on all parties, on or before **July 11, 2013**, written objections that specifically identify the portions of the proposed findings or recommendations to which objection is being made, and a brief in support thereof. A party may respond to the objecting party's brief within fourteen (14) days after service thereof. All briefs filed under the rules shall be limited to 3,500 words. A judge shall make a de novo determination of those portions to which objection is made.

Unless the parties are prepared to stipulate that the District Court is not required by 28 U.S.C. § 636 to review a transcript of the hearing in order to resolve all objections made to this Report and Recommendation, the party making the objections shall timely order and cause to be filed by **July 11, 2013,** a complete transcript of the hearing.

This Report and Recommendation does not constitute an order or judgment of the District Court, and it is, therefore, not appealable to the Circuit Court of Appeals.